ABSTRACT FOR JP2003-521062

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
2. August 2001 (02.08.2001)

PCT

(10) Internationale Veröffentlichungsnummer
WO 01/55836 A1

(51) Internationale Patentklassifikation[7]: G06F 7/58

(21) Internationales Aktenzeichen: PCT/DE01/00111

(22) Internationales Anmeldedatum:
12. Januar 2001 (12.01.2001)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
100 03 472.1 27. Januar 2000 (27.01.2000) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: INFINEON TECHNOLOGIES AG [DE/DE]; St.-Martin-Stasse 53, 81669 München (DE).

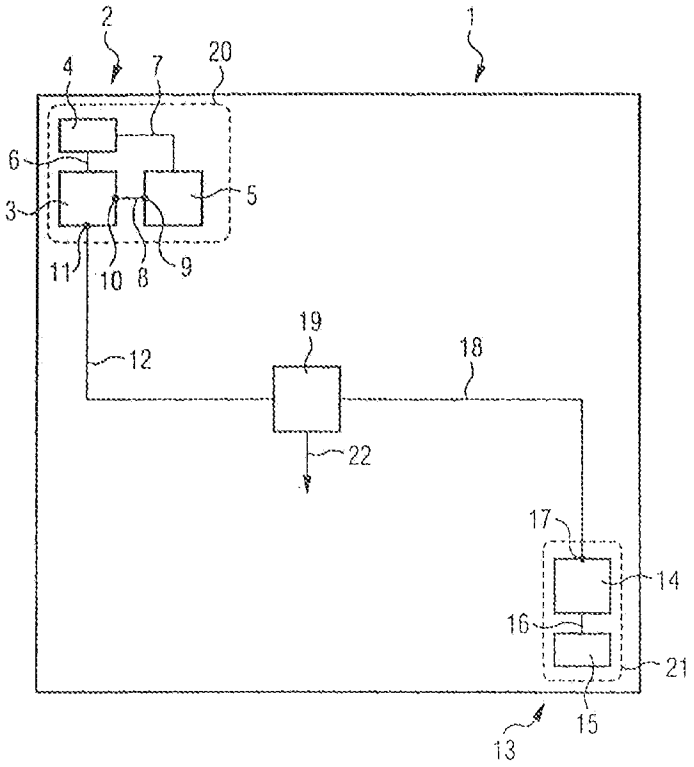
(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: JANSSEN, Norbert [DE/DE]; Innere Wiener Strasse 13A, 81667 München (DE).

(74) Anwalt: EPPING HERMANN & FISCHER; Postfach 12 10 26, 80034 München (DE).

[Fortsetzung auf der nächsten Seite]

(54) Title: RANDOM NUMBER GENERATOR

(54) Bezeichnung: ZUFALLSZAHLENGENERATOR



(57) Abstract: The invention relates to a random number generator on an integrated circuit (1), comprising a first clock generator circuit (2) with a first voltage supply (4), for producing a first signal with a first frequency or a first frequency range; a second clock generator circuit (13) with a second voltage supply (15), for producing a second signal with a second frequency or a second frequency range which is or whose average is lower than the first frequency; and a generator (19) in which the first signal can be sampled with the second signal and which can generate a random number according to the sampling result. The invention is characterized in that the clock generator circuits (2, 13) are situated as far apart as possible from each other on the integrated circuit (1) and/or the two voltage supplies (4, 15) are separated from each other and/or at least one guard ring (20, 21) is placed around each of the clock generator circuits (2, 13).

(57) Zusammenfassung: Die Erfindung ist gerichtet auf einen Zufallszahlengenerator auf einem integrierten Schaltkreis (1) mit einer ersten Taktgeberschaltung (2) mit einer ersten Spannungsversorgung (4) zur Erzeugung eines ersten Signals einer ersten Frequenz oder eines ersten Frequenzbereichs;

[Fortsetzung auf der nächsten Seite]

WO 01/55836 A1

(19)日本国特許庁（ＪＰ）　(12) **公表特許公報**（Ａ）　(11)特許出願公表番号
特表2003－521062
（P2003－521062A）
(43)公表日　平成15年７月８日(2003.7.8)

(51)Int.Cl.[7]	識別記号	Ｆ Ｉ		テーマコード(参考)
Ｇ０６Ｆ　7/58		Ｇ０６Ｆ　7/58	Ｚ	５Ｆ０３８
1/04		1/04	Ｃ	５Ｊ０４９
Ｇ０９Ｃ　1/00	６５０	Ｇ０９Ｃ　1/00	６５０Ｂ	５Ｊ１０４
Ｈ０１Ｌ　21/822		Ｈ０３Ｋ　3/84	Ｚ	
27/04		Ｈ０４Ｌ　9/00	６２１Ｚ	

審査請求　有　　予備審査請求　有　（全 20 頁）　最終頁に続く

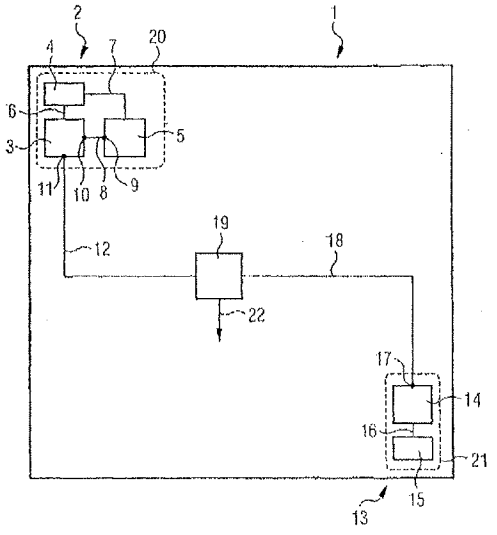
(21)出願番号　特願2001－555316(P2001－555316)
(86)(22)出願日　平成13年１月12日(2001.1.12)
(85)翻訳文提出日　平成14年７月26日(2002.7.26)
(86)国際出願番号　ＰＣＴ／ＤＥ０１／００１１１
(87)国際公開番号　ＷＯ０１／０５５８３６
(87)国際公開日　平成13年８月２日(2001.8.2)
(31)優先権主張番号　１００　０３　４７２．１
(32)優先日　平成12年１月27日(2000.1.27)
(33)優先権主張国　ドイツ（ＤＥ）
(81)指定国　ＥＰ(ＡＴ，ＢＥ，ＣＨ，ＣＹ，ＤＥ，ＤＫ，ＥＳ，ＦＩ，ＦＲ，ＧＢ，ＧＲ，ＩＥ，ＩＴ，ＬＵ，ＭＣ，ＮＬ，ＰＴ，ＳＥ，ＴＲ)，ＢＲ，ＣＡ，ＣＮ，ＩＬ，ＩＮ，ＪＰ，ＫＲ，ＭＸ，ＲＵ，ＵＡ，ＵＳ

(71)出願人　インフィネオン　テクノロジーズ　アクチェンゲゼルシャフト
ドイツ連邦共和国，デーー81669　ミュンヘン，ザンクトーマルティンーシュトラーセ　53
(72)発明者　ヤンセン，　ノルベルト
ドイツ国　81667　ミュンヘン，　インネレ　ヴィナー　シュトラーセ　13アー
(74)代理人　弁理士　山本　秀策　（外２名）

Ｆターム(参考)　5F038 AZ03 BG02 BG06 BH09 BH19 CA07 CD06 DF01 EZ20
5J049 AA01 AA03 AA17 AA18 CA09
5J104 FA10 NA04

(54)【発明の名称】　乱数生成器

(57)【要約】
本発明は、集積回路（１）上の乱数生成器に関する。上記乱数生成器は、第１の周波数または第１の周波数の範囲によって第１の信号を生成する第１の電圧供給源（４）を有する第１のクロック生成器の回路（２）と、第２の周波数または第２の周波数の範囲で第２の信号を生成する第２の電圧供給源（１５）を有する第２のクロック生成器の回路（１３）であって、上記第２の周波数または上記第２の周波数の範囲またはその平均値は上記第１の周波数より低い、第２のクロック生成器の回路と、生成器（１９）であって、上記生成器（１９）において、上記第１の信号は上記第２の信号によってサンプリングされ得、そして上記サンプリングの結果によって乱数を生成し得る生成器とを含む。



【特許請求の範囲】

【請求項１】　集積回路（１）上の乱数生成器であって、第１の周波数または第１の周波数の範囲の第１の信号を生成する第１の電圧供給源（４）を有する第１のクロック生成器の回路（２）と、第２の周波数または第２の周波数の範囲の第２の信号を生成する第２の電圧供給源（１５）を有する第２のクロック生成器の回路（１３）であって、該第２の周波数または該第２の周波数の範囲またはその平均値は該第１の周波数より低い、第２のクロック生成器の回路（１３）と、生成器（１９）であって、該生成器（１９）において、該第１の信号は該第２の信号によってサンプリングされ得、そして少なくとも１つの乱数を該サンプリングの結果に依存する様態で生成し得る生成器（１９）とを含み、該クロック生成器の回路（２、１３）は該集積回路（１）上で相互からできるだけ離れて配置されており、および／または該２つの電圧供給源（４、１５）は相互から分離されており、および／または少なくとも１つの保護リング（２０、２１）は該クロック生成器の回路（２、１３）のそれぞれの周囲に配置されていることを特徴とする乱数生成器。

【請求項２】　前記クロック生成器の回路（２、１３）は前記集積回路（１）上で相互からできるだけ離れて配置されており、そして前記２つの電圧供給源（４、１５）は相互から分離されており、そして少なくとも１つの保護リング（２０、２１）は該クロック生成器の回路（２、１３）のそれぞれの周囲に配置されていることを特徴とする、請求項１に記載の乱数生成器。

【請求項３】　前記クロック生成器の回路は、前記集積回路（１）上に該集積回路上で対角線上の相互に対向する角の領域内にあるように配置されていることを特徴とする、請求項１または２に記載の乱数生成器。

【請求項４】　前記電圧供給源（４、１５）は少なくとも１つのＲＣ素子によって分離されていることを特徴とする、請求項１、２および３のいずれかに記載の乱数生成器。

【請求項５】　両方の電圧供給源（４、１５）はそれぞれＲＣ素子によって分離されていることを特徴とする、請求項４に記載の乱数生成器。

【請求項６】　前記クロック生成器の回路（２、１３）のうちの１つを分離

する前記ＲＣ素子の非干渉周波数は、それぞれまたは他のクロック生成器の回路（２、１３）の前記信号の周波数の範囲の平均値に対応することを特徴とする、請求項４または５に記載の乱数生成器。

【請求項７】　前記電圧供給源（４、１５）は少なくとも１つの電圧調整器によって分離されていることを特徴とする、請求項１～６のいずれかに記載の乱数生成器。

【請求項８】　前記第１の信号は変化する周波数を有することを特徴とする、請求項１～７のいずれかに記載の乱数生成器。

【請求項９】　前記第２の信号は変化する周波数を有することを特徴とする、請求項１～８のいずれかに記載の乱数生成器。

【請求項１０】　前記第２の信号は前記第１の信号の周波数より少なくとも１０倍低い周波数を有することを特徴とする、請求項１～９のいずれかに記載の乱数生成器。

【請求項１１】　前記第２の信号は前記第１の信号の周波数より少なくとも１００倍低い周波数を有することを特徴とする、請求項１０に記載の乱数生成器。

【請求項１２】　前記生成器（１９）は乱数の連続を生成することを特徴とする、請求項１～１１のいずれかに記載の乱数生成器。

【請求項１３】　前記生成器（１９）は、一定ではない電力の補正および／または乱数生成器の重み付けの等化回路（３２）をさらに有することを特徴とする、請求項１～１２のいずれかに記載の乱数生成器。

【請求項１４】　前記等化回路（３２）は線形のフィードバックシフトレジスタを有することを特徴とする、請求項１３に記載の乱数生成器。

【請求項１５】　前記第１および／または前記第２のクロック生成器の回路（２、１３）は、少なくとも１つの電圧結合発振器（３、２３、２５、２６）およびさらなる発振器（５、２４、２７）を有し、該発振器の信号出力（９）は該電圧結合発振器（３、２３、２５、２６）の制御入力（１０）に接続されていることを特徴とする、請求項１～１４のいずれかに記載の乱数生成器。

【請求項１６】　前記さらなる発振器は電圧結合発振器（２３、２４、２６

、２７）であり、該発振器の制御入力は定電圧に接続されていることを特徴とする、請求項１５に記載の乱数生成器。

【請求項１７】　前記第１および／または前記第２のクロック生成器の回路は、複数の直列に接続された電圧結合発振器を有し、該電圧結合発振器の該直列の最後を除くそれぞれの信号出力は、次の電圧結合発振器の制御入力に接続されていることを特徴とする、請求項１５または１６に記載の乱数生成器。

【発明の詳細な説明】

【０００１】

本発明は、乱数を生成する回路構成に関し、具体的には、集積回路上の乱数生成器の回路の構成に関する。

【０００２】

乱数の生成は、科学および技術の多くの分野において非常に重要である。したがって、乱数は、統計における多数の用途および暗号目的に必要である。データネットワークの普及および関連付けられたセキュリティの問題において重要性がますます高まってきているのがまさに暗号法である。したがって、乱数の自動生成は、電子エンジニアリングおよびエレクトロニクス、特にデータ処理において重要な分野を成す。乱数の生成だけでなく、乱数の質も重要である。すべての方法が均一に「ランダム」である乱数を生成し得るわけではない。むしろ、通常は、特定の乱数生成器によって生成された大多数の乱数を分析して、生成された数の理想的でランダムな分布から偏差につながるパターンを識別することが可能である。乱数の質の測定は、Ｓｈａｎｎｏｎによって「Ａ　Ｍａｔｈｅｍａｔｉｃ　Ｂｅｌｌ　Ｓｙｓｔｅｍ　Ｔｅｃｈｎｉｃａｌ　Ｊｏｕｒｎａｌ、ｖｏｌ．２７、ｐ．３７９（１９４８年）に記載されるように、乱数のエントロピーである。

【０００３】

従来技術における公知の乱数を生成する方法は、高周波を有する信号を著しく低い周波数を有する第２の信号によってサンプリングすることを含む。したがって、これらの信号は、特定の出力に存在し、２つの振幅値の間で振動し、そして時間的なプロファイルにおいて特定の速度で振動する電圧である。サンプリングは、両方の信号が供給される特定の回路内で実行される。この場合、第２の信号の波プロファイルの特定の点が常に用いられて、第１の信号がサンプリングされる瞬間を決定する。すなわち、信号の値（例えば、電圧として測定される値）が確認されて、数値に変換される。

【０００４】

デジタル回路において、これらの数値は、最も簡単な場合には、０または１の

値である。例えば、サンプリングの瞬間に、第１の信号の波の進路（ｗａｖｅ　ｃｏｕｒｓｅ）が平均値（例えば、０ボルト）よりも高い場合には「１」、そして波の進路が平均値よりも低い場合には「０」である。しかし、得られた値を継続的に解釈して、均一なアナログ数値（例えば、１：１の数値に変換されたミリボルトの電圧）を得ることが可能である。

【０００５】

２つの信号の理想的な波の進路の場合、振幅値のサンプリングにおいて周期性を観察することが可能であり、この周期性は２つの周波数比により生じる。結果的に、このような乱数生成器の支援によっては、真の乱数を生成することは可能ではない。しかし、実際には、２つの信号の波は理想的な波の進路ではなく、むしろ、正確にはマイクロエレクトロニクスの分野においては不可避なノイズに起因して誤差が波の進路において生じる。このため、うまく機能する乱数生成器は、信号が相互から独立している場合に、わずかに２つの簡単な所定の周波数によって達成され得るという影響を有し得る。

【０００６】

しかし、実際には、このような簡単な乱数生成器は、生成される乱数の質から成る高い要件を満たしてはいない。これは、２つの信号が相互から独立していることが乱数の質にとって本質的に重要だからである。これは、１つの信号が用いられる回路内にある電気信号パスを通る他の信号の影響を受けず、その結果、２つの信号が特定の様態で相互に結合されることを意味する。

【０００７】

上述の原理に対応するいわゆる物理ノイズ生成器において、例えば、サンプリングされる信号（すなわち、一定ではない周波数を有する第１の信号）によって、２つの信号のこの独立性の問題を解決する試みが行われた。サンプリングされるこのような信号は、例えば、乱数を生成する回路（いわゆる電圧結合発振器（電圧制御発振器、ＶＣＯ）であり、このＶＣＯの制御入力は、例えば、第２の発振器によって提供されるような周期的に変化する信号によって供給される）内に統合することによって得られ得る。この結果、これは、ＶＣＯの信号の周波数が第２の発振器の波の進路に依存する様態で変調されるような影響を有する。この

場合、第２の発振器はさらに、一定の周波数を有する振動信号が発振器の信号出力において出力されるように、例えば、発振器の制御入力において定電圧で動作するＶＣＯであってもよい。しかし、このアプローチであっても依然、使用するすべての分野において満足ゆく結果が得られない。結果、２つの信号が一時的に結合され、これにより、第１の信号の周波数が特定の時間点におけるこのような結合に適し、２つの信号が特定の時間の後に再度相互から分岐する場合、混合された周波数が形成されることが生じ得る。この結果、回路によって提供された乱数の質が第１の信号の変化する周波数によって振動する。したがって、生成される乱数の質がよりよい乱数生成器を依然必要とする。

【０００８】

ＤＤ２７９　７６３　Ａ１号は、その周波数が少なくとも係数１００だけ異なる、２つの相互に関連付けられていない電気発振器が用いられるマイクロコンピュータにおいて乱数を生成する方法を記載する。発振器は２つの独立したソースによって、正確には、周波数間にも、２つの振動の位相角間にも相関がないような方法で生成される。より高い周波数の振動は、マイクロコンピュータによって開始されるカウンターによってカウントされ、そしてカウンターを停止するには、より低い周波数の振動が用いられる。次いで、さらなる処理のカウンター読み取りを行うように、カウンターが停止した後、乱数が利用可能になる。

【０００９】

ＵＳ５，８５９，５４０号は、光ダイオードの暗電流を減少させるために設けられた保護リングを記載する。欄４内の記載によると、この場合に含まれるのは、空乏ゾーンの位置を変更し、したがって、暗電流を減少させる、半導体材料中の環状で高くドーピングされた領域である。保護リングは概して、電流の限界を決定する目的でコンポーネントを包囲する半導体材料中のドーピングされた領域である。

【００１０】

したがって、本発明は、２つの信号が従来公知であったものより良好な程度に独立していることが保証されている汎用タイプの乱数生成器を提供する目的に基づく。この目的は、特許請求の範囲の独立項１による乱数生成器によって達成さ

れる。本発明のさらに有利な改良点、局面および詳細は、従属項、説明および添付の図面から生成される。

【００１１】

本発明は、個々または組合せて、乱数生成器の２つの信号の独立性を明瞭に高め得る一連の手段を提供する原理に基づく。

【００１２】

したがって、本発明は概して、集積回路上の乱数生成器に関する。乱数生成器は、第１の周波数または第１の周波数の範囲の第１の信号を生成する第１の電圧供給源を有する第１のクロック生成器の回路と、第２の周波数および第２の周波数の範囲の第２の信号を生成する第２の電圧供給源を有する第２のクロック生成器の回路であって、第２の周波数および第２の周波数の範囲またはその平均値は第１の周波数より低い、第２のクロック生成器の回路と、生成器であって、生成器において、第１の信号は第２の信号によってサンプリングされ得、そして少なくとも１つの乱数をサンプリングの結果に依存する様態で生成し得る生成器とを含み、クロック生成器の回路は集積回路上で相互からできるだけ離れて配置されており、および／または２つの電圧供給源は相互から分離されており、および／または少なくとも１つの保護リングはクロック生成器の回路のそれぞれの周囲に配置されていることを特徴とする。

【００１３】

第１のクロック生成器の回路は、サンプリングされる信号を供給し、したがって、固定周波数を生成し得るか、または所定の周波数の範囲で変化する変化する周波数を出力し得る。固定周波数の最も簡単な場合は、従来技術としてすでに上述しており、乱数がコンポーネント内の不可避なノイズの結果にもかかわらず、生成され得るという原理に基づく。全周波数の範囲の使用、すなわち、変化する周波数を有する信号の出力は、従来技術における最新の技術である。

【００１４】

同じことが第２のクロック生成器の回路に適用される。第２のクロック生成器の回路は通常、固定周波数であるが、変化する周波数の第２の信号を特定の周波数の範囲で構成することも等しく可能であり得る。この場合、単位時間ごとに生

成される乱数の数は、第２の信号の周波数で変動し得る。しかし、この構成は、乱数の質を向上させる利点を有し得る。

【００１５】

上に概要を述べたように、生成器は時間的なプロファイルの評価および２つの信号の値を介して乱数を生成する。最も簡単な場合、生成器は、第１の信号が供給される入力内にフリップフロップされ得、そしてこの出力は、例えば、制御入力に存在する第２の信号が立ち上がり端を有する場合に、新たな値に常に接続される。このような回路の対応する実現は当業者に知られている。

【００１６】

集積回路上の２つのクロック生成器の回路を最大に可能な距離だけ分離すると、２つの信号の相互に対する影響を距離によって減少させる効果がある。これにより、集積回路の全サイズに依存して、変化する質の結果を得ることが可能である。この場合、「相互からできるだけ離れて」は２つのクロック生成器の回路を形成するコンポーネントが、集積回路の他の回路部の状態を考慮して相互から極端に遠くに、例えば、集積回路の対角線上の対向する角内に存在することを意味すると理解される。

【００１７】

本発明による電圧供給源の分離は、信号が電圧供給源の電流（結合した２つの信号の周波数の従来のパスを表す）上にクロストークを発生させ得ないという効果を有する。

【００１８】

最後に、保護リングも同様に、集積回路を介して信号の伝播を防ぐことを助ける。

【００１９】

特に、提案された手段のうちの２つまたはさらには３つすべてを本発明による集積回路上の乱数生成器内に同時に実現することが好適である。これらの手段すべては、信号の独立性を高めることに貢献する。

【００２０】

電圧供給源は、好適には、少なくとも１つのＲＣ素子によって分離され得る。

ＲＣ素子は、特定の狭い周波数の範囲内の信号のみが通過することを可能にし、そして他の周波数を阻止するアセンブリである。したがって、結局は異なる周波数を有する他の信号を、それぞれの他のクロック生成器の回路内への入力部において効果的に妨害し得るＲＣ素子を選択することが可能である。クロック生成器の回路から信号の出力を防ぐようにＲＣ素子の寸法調整することも可能である。出力周波数が変化する周波数である場合、存在する周波数の平均値が伝送されるようにＲＣ素子を選択することが適切である。電圧供給源のうちに１つをフィルタリングするＲＣ素子を用いることは十分であり得るが、ＲＣ素子はそれぞれ、クロック生成器の回路それぞれに設けられ得て、クロック生成器の回路を分離することが好適である。

【００２１】

ＲＣ素子の使用の代わりまたはＲＣ素子の使用に加えて、電圧供給源を少なくとも１つの電圧調整器によって分離することも可能であり得る。この場合、次いで、両方のクロック生成器の回路は第１に共通の電圧供給源によって供給され得るが、共通の電圧供給はそれぞれの電圧調整器を介して流れる。この電圧調整器も、その設計に起因して、信号の分離を可能にする。

【００２２】

本発明は、第１の信号が変化する周波数を有するか、または第２の信号が変化する周波数を有することを特徴とし得る。すでに上に説明したように、これは、周波数が、対応するコンポーネントを用いることによって周期的に変化することを可能にする可能性に関する。

【００２３】

従来技術の説明にすでに述べたように、第２の信号の周波数は第１の信号の周波数より著しく低いことが利点である。特に、第２の信号が第１の信号の周波数よりも少なくとも１０倍低い周波数を有することが好適であり、特に好適には、第１の信号の周波数より少なくとも１００倍低い周波数を有する。

【００２４】

周波数を選択すると、第２の信号のいわゆるジッター（特定の信号状態の一時的な発生の変形）を得ることが可能になる。このジッターは、第１の信号のより

ランダムなサンプリングが可能であるように、複数の第１の信号の振動をカバーする。

【００２５】

生成器は少なくとも１つの乱数を生成する。しかし、クロック生成器の回路が連続信号を供給するため、生成器が連続的に乱数を生成することが適切であり、そして好適である。事実、かなり一般的には、それぞれの場合に、数値または数値のディジットを供給する第２の信号の波の進路における特定の領域の到達点に依存して、乱数のストリームが生成される。例として、生成器が０および１を含むバイナリ数値を生成するように生成器を設計して、そしてそれぞれの場合にこれらのバイナリ値の所定の数値が全乱数を形成するように組み合わせることが可能である。

【００２６】

したがって、例えば、１６または３２のバイナリ数値を組み合わせて、１６または３２ビットの適切な乱数を形成することが可能である。

【００２７】

上述したように、生成器は簡単な実施形態において単なるフリップフロップを含み得る。しかし、これは、本発明による手段にも関わらず、生成器が、例えば、第２の信号の一定ではない周波数に起因して、乱数の生成中に一定ではない電力を供給するという効果を有し得る。さらに、乱数は特定の値に対して影響を受け得る。すなわち、固有の重み付けを有し得る。したがって、生成器がさらに、一定ではない電力の補正および／または乱数生成器の重み付けの等化回路を有することが好適である。第１の信号をサンプリングする第２の信号がさらに、フローティングプロファイル（すなわち、最小値と最大値との間で周期的に変化する周波数）を有する場合、乱数生成器の電力も周波数によって変化する。これは、例えば、フィードバックシフトレジスタ（これに対して、乱数生成器の出力信号が供給される）によって実現され得る好適な等化回路によって補正され得る。公知であるように、シフトレジスタは、エントロピー格納装置である。信号（例えば、ビット）がシフトレジスタから、乱数生成器の最小の出力信号速度以下の一定の速度で取り出された場合、取り出された信号ストリーム（例えば、ビットス

トリーム）は、乱数生成器からの信号ストリームのエントロピー以上のエントロピーを有する。しかし、生成された乱数の質を高めることに役立つ回路上の他の処理後の方法も考えられる。

【００２８】

さらに好適な実施形態において、第１および／または第２のクロック生成器の回路は、少なくとも１つの電圧結合発振器およびさらなる発振器を有し得、この発振器の信号出力は、電圧結合発振器の制御入力に接続される。基本的に公知であるこの構成は、本発明と組み合わされないが、乱数の質をさらに高めることを可能にする。さらなる発振器はさらに、電圧結合発振器でもあり得、この発振器の制御入力は定電圧に接続される。このように、電圧結合発振器は、１つの周波数のみを出力する１つの発振器のように動作する。電圧結合発振器が用いられた場合、より少ないコンポーネントまたはアセンブリの種類しか必要でないため、回路は全体的に簡略化され得る。

【００２９】

生成された乱数の質をさらに高めるには、第１および／または第２のクロック生成器の回路が複数の直列に接続された電圧結合発振器を有し、電圧結合発振器の直列の最後を除くそれぞれの信号出力は、次の電圧結合発振器の制御入力に接続されていることも同様に好適であり得る。このように、第２の信号によるサンプリングの周期性がさらに増加するように、第１の信号の出力においてさらにより複雑な周波数のパターンを得ることが可能である。

【００３０】

本発明の具体的な例示の実施形態を、以下を示す添付の図面を参照しながら以下に記載する。

【００３１】

図１は、概して、第１のクロック生成器の回路２および第２のクロック生成器の回路１３を有する集積回路１を示す。第１のクロック生成器の回路２は、第１の信号のクロック生成器３、および第１のクロック生成器の電圧供給源４を有する。この例において、第１のクロック生成器の回路２によって生成される第１の信号の周波数は変化することが意図され、これにより、第１の信号のクロック生

成器３は、例えば、ＶＣＯである。このＶＣＯの制御入力１０に対しては、第１のクロック生成器の回路２のさらなる発振器５が接続され、このさらなる発振器５は、制御入力１０に信号出力９および信号線８を介して一定の周波数を有する信号を供給する。

【００３２】

第２のクロック生成器の回路１３は、第２の信号のクロック生成器１４を有する。クロック生成器１４は、本発明のより簡単な例示の実施形態において、例えば、一定の周波数を有する発振器であってもよい。発振器は、第２のクロック生成器の電圧供給源１５および電圧供給線１６を介して適切な動作電圧を供給される。第１のクロック生成器の回路２は、第１の信号の信号出力１１を介して信号を出力し、この信号は、第１の信号の信号線１２を介して乱数生成器に供給される。同様に、第２の信号のクロック生成器１４は、第２の信号を、第２の信号の信号出力１７および信号線１８を介して乱数生成器１９に出力する。乱数生成の後、乱数生成器１９は乱数出力２２を介して乱数を出力する。

【００３３】

第１のクロック生成器の回路２はさらに電圧供給源４を有する。電圧供給源４は、クロック生成器に、電圧供給線６、７を介してエネルギーを供給する。第２のクロック生成器の回路１３には第２の電圧供給源が設けられる。第２の電圧供給源は、クロック生成器１４に、電圧供給線１６を介してエネルギーを供給する。

【００３４】

本発明によれば、２つのクロック生成器の回路２および１３は、集積回路１上で相互からできるだけ離れて配置されるように構成される。これは、対応するアセンブリを集積回路の対角線上の対向する角に配置することによって保証される。しかし、任意の他の方法で技術的に可能でない場合、クロック生成器の回路の構成に他の位置を用いることも可能である。

【００３５】

さらに、本発明による保護リングは、２つのクロック生成器の回路のそれぞれの周囲に配置される。以下の例において、ｐ－ドーピング型またはＮドーピング

型の保護リング２０は、第１の信号のクロック生成器の回路２の周囲に配置され、同一にドーピングされた保護リング２１は第２のクロック生成器の回路１３の周囲に配置される。

【００３６】

最後に、本発明によれば、２つの電圧供給源４および１５は上述の手段（例示しない）によって相互から分離され得る。

【００３７】

図２は、本発明のより複雑な例示の実施形態を示す。この場合、第１のクロック生成器の回路２は、全部で３つのＶＣＯを有する。３つのＶＣＯとは、すなわち、第１の信号のクロック生成器３、第１の信号の第２のＶＣＯ２３、および第１の信号の第３のＶＣＯ２４であり、これらはすべて、電圧供給源４によって電圧供給線６、７を介して電圧を供給される。

【００３８】

第３のＶＣＯ２４は、第３のＶＣＯ２４の信号出力３０および信号線２９を介して、第２のＶＣＯ２３の制御入力３１に一定の周波数を有する信号を出力する。ＶＣＯ２３は、引き続いて、信号出力９において、信号線８を介して第１のクロック生成器３の制御入力１０に、変化する周波数を有する信号を出力する。したがって、第１のクロック生成器はより複雑な信号を生成し、この信号は上述したように乱数生成器１９に転送される。本発明の例示の実施形態において、同じ構成が第２の信号の生成にも用いられる。この場合、電圧供給線１６および２８を介してエネルギーを供給される３つのＶＣＯ２５、２６および２７が用いられる。

【００３９】

本発明によって構成された乱数生成器により、以前に公知の回路によって可能であったものより相当、質が向上した乱数を生成することが可能になる。提案された解決策が驚くほど簡潔であるため、本発明による乱数生成器の具体的な実現においてより費用効果のある実現が可能になる。

【図面の簡単な説明】

【図１】

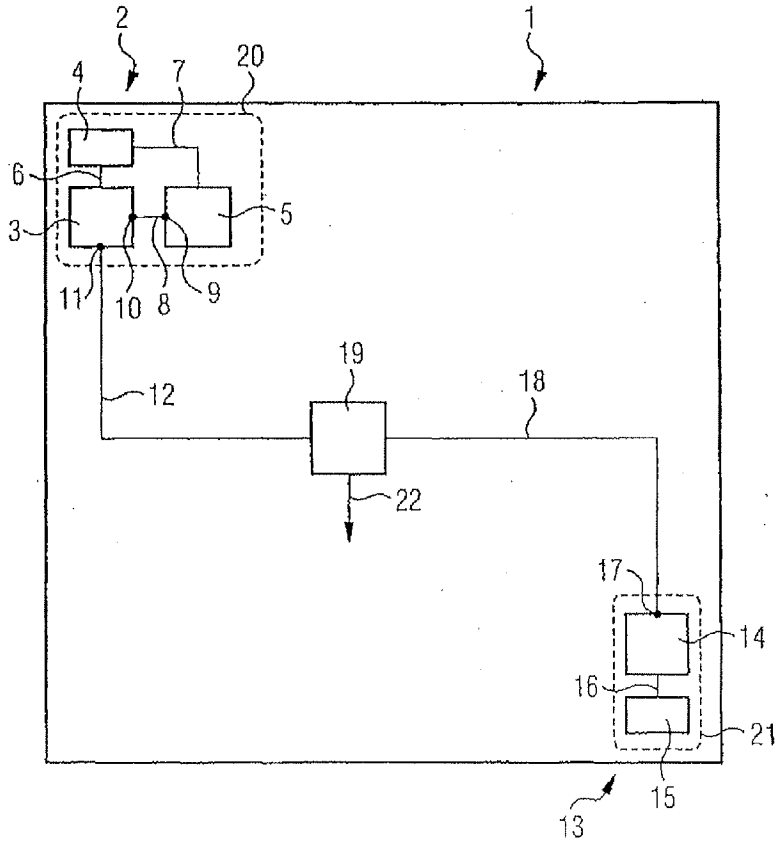
図１は、本発明によるより簡単な実施形態における、２つのクロック生成器の回路を有する乱数生成器を示す。

【図２】

図２は、本発明による、より複雑なクロック生成器の回路構成を示す。

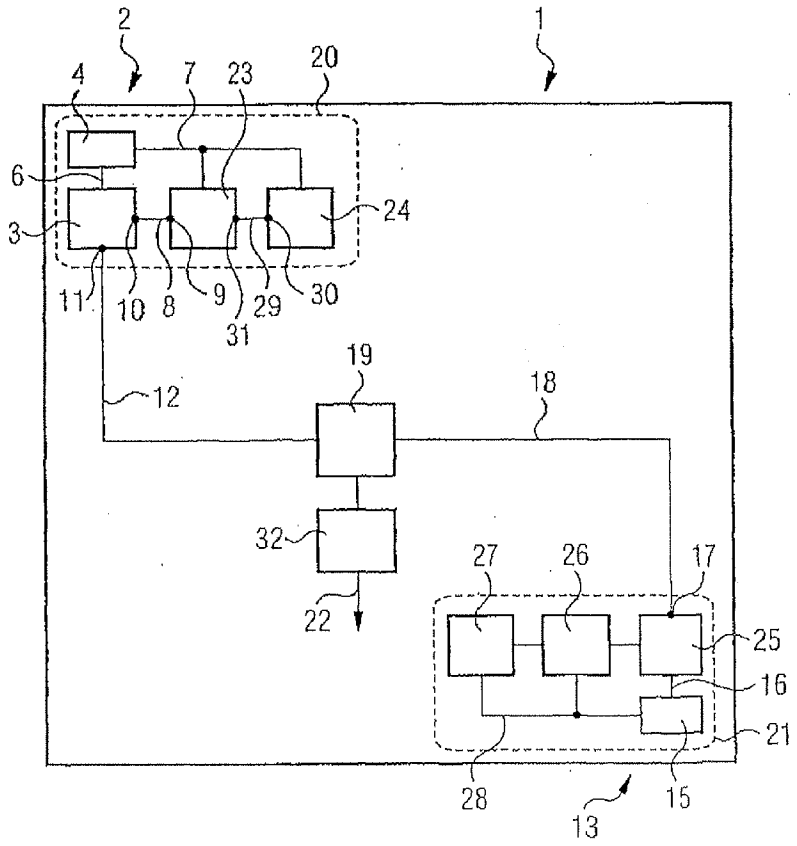
【図１】

FIG 1



【図２】

FIG 2


2
1
4
7
23
20
6
3
24
11
10
8
9
29
30
31
12
19
18
32
22
27
26
17
25
16
21
28
13
15

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International Application No
PCT/[ ]1/00111

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F7/58

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	"INTEGRATED CIRCUIT COMPATIBLE RANDOM NUMBER GENERATOR" IBM TECHNICAL DISCLOSURE BULLETIN,US,IBM CORP. NEW YORK, vol. 30, no. 11, 1 April 1988 (1988-04-01), pages 333-335, XP000021682 ISSN: 0018-8689 page 334, paragraph 2 ---	1-17
Y	DD 279 763 A (THAELMANN SCHWERMASCHBAU VEB) 13 June 1990 (1990-06-13) cited in the application the whole document ---	1-17
	-/--	

[X] Further documents are listed in the continuation of box C. [X] Patent family members are listed in annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 June 2001	04/07/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Cohen, B

Form PCT/ISA/210 (second sheet) (July 1992)

page 1 of 2

INTERNATIONAL SEARCH REPORT

International Application No
PCT/I 11/00111

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
Y	MURRY: "A General Approach for Generating Natural Random Variables" IEEE TRANSACTIONS ON ELECTRONIC COMPUTERS., vol. c-19, no. 12, December 1970 (1970-12), pages 1210-1213, XP002169916 IEEE INC. NEW YORK., US Seite 1213, Absatz "Recommendations..."	1-17
A	US 5 010 331 A (DIAS DONALD R ET AL) 23 April 1991 (1991-04-23) abstract column 5, line 8 - line 19 column 24, line 1 - line 47 column 33, line 4 - line 12	1
A	PETRIE C S ET AL: "MODELING AND SIMULATION OF OSCILLATOR-BASED RANDOM NUMBER GENERATORS" IEEE INTERNATIONAL SYMPOSIUM ON CIRCUITS AND SYSTEMS (ISCAS),US,NEW YORK, IEEE, 12 May 1996 (1996-05-12), pages 324-327, XP000704602 ISBN: 0-7803-3074-9 paragraph '04.3!; figure 1	1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/I 01/00111

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
DD 279763	A	13-06-1990	NONE		
US 5010331	A	23-04-1991	US	4935645 A	19-06-1990
			US	4897860 A	30-01-1990
			US	4870401 A	26-09-1989
			US	5838256 A	17-11-1998
			US	4943804 A	24-07-1990

Form PCT/ISA/210 (patent family annex) (July 1992)

フロントページの続き

(51) Int.Cl.[7]	識別記号	F I	テーマコード（参考）
H03K 3/84		H01L 27/04	H
H04L 9/10			